Department of Homeland Security
IAIP Directorate
Daily Open Source Infrastructure Report
for 29 April 2004

Current Nationwide Threat Level is
ELEVATED
Significant Risk of Terrorist Attacks
For info click here
www.whitehouse.gov/homeland

Daily Overview

- TCPalm.com reports six security guards and a supervisor have been removed from duty at the St. Lucie Nuclear Plant after a Florida Power & Light Co. audit found the guards failed to complete their patrols. (See item 1)
- EurekAlert reports researchers say airport baggage screeners may need continuing education in otder to identify potentially new and unexpected weapons. (See item 10)
- MSNBC reports Food and Drug Administration records indicate almost 100 U.S. companies have recently violated regulations meant to prevent the spread of mad cow disease. (See item 19)

DHS/IAIP Update *Fast Jump*

Energy Sector

Current Electricity Sector Threat Alert Levels: Physical: Elevated, Cyber: Elevated
Scale: LOW, GUARDED, ELEVATED, HIGH, SEVERE [Source: ISAC for the Electricity Sector (ES−ISAC) − http://esisac.com]

1. *April 28, TCPalm.com* — **St. Lucie nuclear plant guards removed from duty. Six security guards and a supervisor have been removed from duty at the St. Lucie Nuclear Plant after a Florida Power & Light Co. audit found the guards failed to complete their patrols, a Wackenhut Corp. official said Tuesday, April 27. The audit revealed the guards skipped parts of their rounds at the plant, and took shortcuts during patrols designed to detect and prevent fires.** FPL launched its audit in March, after a security officer told plant managers certain guards were not completing their patrols, said FPL spokesperson Rachel Scott. FPL

examined computer records tracking the location of guards and discovered some had not covered all their assigned areas. Scott said FPL had "no tolerance" for such oversights. Because the plant uses many different security measures, including electronic and video surveillance, Scott said the lapses did not compromise security. Since March, FPL has installed a more sophisticated patrol−monitoring system that tracks the location of guards in real−time. It also clarified its expectations and requirements of Wackenhut guards, Scott said. The St. Lucie Nuclear Plant is located near Ft. Pierce, FL.
Source: http://www.tcpalm.com/tcp/local_news/article/0,1651,TCP_1673 6_2842623,00.html

2. *April 28, Associated Press* — **Power outages linger from spring storm. Thousands of northwest Washington residents remained without electricity Wednesday, April 28, after a wind storm brought lightning, hail and a report of a rare tornado touching down east of Sumas, near the Canadian border.** About 200,000 homes and businesses lost power at the height of the storm Tuesday, April 27, when sustained winds of 45 mph buffeted the region. Mike Thorne of the Snohomish County Public Utilities District said about 40,000 customers were still without power Wednesday. Spokesperson Tim Bader or Puget Sound Energy said it had about 12,000 customers without service, down from about 50,000 outages at the storm's peak. About 9,900 customers lost power in Seattle City Light's coverage area and another 5,600 customers were out in Tacoma, spokespersons said.
Source: http://www.kgw.com/sharedcontent/APStories/stories/D827QTCG0 .html

3. *April 28, Reuters* — **Natural gas prices may not drop as expected. U.S. natural gas prices are expected to hover near record highs this year, and not drop as originally forecast, as sagging domestic production and a recovering economy keep supplies tight.** Analysts, who last year predicted prices in 2004 would slip 50 to 75 cents from 2003's record high average of $5.43 per mmbtu as producers stepped up drilling, have been forced to raise their estimates. Most now expect this year's price average to come close to matching last year's record heights, primarily due to tight supplies. **Analysts called strained supplies in the United States and Canada the main culprit in the case for near−record high prices this year.** They said output from U.S. gas fields is still struggling and not likely to improve much this year. In addition, Canada is wrestling with dwindling output from mature fields, offering little hope that exports to the U.S., which fell 5 to 7 percent last year, will improve in 2004. The United States relies on Canadian supplies to meet about 15 percent of its total domestic gas demand.
Source: http://msnbc.msn.com/id/4854044/

4. *April 28, PPL Corporation* — **Unusual event declared at PPL's Susquehanna nuclear power plant. PPL's Susquehanna nuclear power plant in Luzerne County declared an "unusual event" at 1:25 p.m. EDT on Wednesday, April 28, because of an electrical failure in a power distribution panel located in the Unit 2 reactor building. The affected distribution panel supplies power to the cooling system for the main generator.** Power also was disrupted to the system that removes certain gases from the turbine's main condenser, without which the unit cannot operate at full power, said Herbert D. Woodeshick, special assistant to the president for PPL Susquehanna. PPL has notified Luzerne and Columbia county emergency management agencies, as well as the Pennsylvania Emergency Management Agency, which are coordinating support services as needed. The company also has notified the Nuclear Regulatory Commission. PPL has activated its Media Operations Center at the Susquehanna Energy Information Center. The Susquehanna plant is located about seven miles

north of Berwick, PA.
Source: http://www1.pplweb.com/newsapp/news_releases.articleview?p_a rtid=2371

[Return to top]

Chemical Industry and Hazardous Materials Sector

5. *April 28, Associated Press* — **River barge leaks toxic chemical. A pungent smell in the Brusly, MS, area has been identified as a sodium hydrosulfide solution. West Baton Rouge Parish 911 director Sharlot Edwards says the smell has been traced to a barge in the Mississippi River.** Edwards says students from Brusly Elementary School and Lukeville Upper Elementary in Brusly were sent home for the day. Officials say the chemical is toxic if it is inhaled, ingested or touches the skin. The chemical is a liquid solution that can be used to remove zinc and mercury from aluminum or to separate copper ores in paper processing and the tanning industry.
Source: http://www.katc.com/Global/story.asp?S=1823112&nav=EyAzMfgP

[Return to top]

Defense Industrial Base Sector

6. *April 28, Washington Post* — **General says missile defense could be ready soon.** The general in charge of the Pentagon's missile defense programs said yesterday that upcoming flight tests are likely to have little bearing on plans to field a national antimissile system later this year. **Air Force Lt. Gen. Ronald T. Kadish, director of the Pentagon's Missile Defense Agency, said top administration and military officials have yet to decide when to declare the system on alert −− that is, ready to engage ballistic missiles fired at the United States. However, he said such a move could come as early as this summer, when the first missile interceptors are installed in newly built silos in Alaska.** The interceptors, along with several ground− and ship−based tracking radars and an extensive network of electronic links, are intended to give the United States the ability to destroy enemy warheads in space by ramming into them. The Bush administration has attached considerable urgency to erecting the antimissile system, citing a growing threat from hostile states trying to acquire long−range missiles. Although two states −− Iraq and Libya −− are no longer the concern that they were, Kadish said the two most worrisome threats remain −− North Korea and Iran.
Source: http://www.washingtonpost.com/wp−dyn/articles/A47651−2004Apr 27.html

[Return to top]

Banking and Finance Sector

7. *April 28, Khaleej Times (United Arab Emirates)* — **Abu Dhabi police busts counterfeit currency racket.** In the United Arab Emirates (UAE), the Criminal Investigation Department (CID) of Abu Dhabi Police, in cooperation with Dubai Police, has broken up the biggest ever counterfeit crime in the country in which a four−member gang was trying to put into circulation fake currency notes worth US$2.7 million, officials said on Tuesday, April 27. Acting on a

tip−off, CID personnel arrested the gang, all Africans, and seized a large amount of counterfeit U.S. dollars, UAE dirham, Euros, stamps, printing machines, copiers and scanners from them, said Colonel Abdul Karim Mohammed Al Marzouqi, Head of Investigation at the Security Affairs Department of the General Directorate of Abu Dhabi Police. **The police recovered counterfeit currency notes worth Dh7 million, US$324,000, and 7,500 Euros in addition to genuine notes used for counterfeiting. The recovered amounts included uncut printed notes. Fake international driving licenses were also seized.** The gang members also had in their possession millions of defaced notes used in black magic operations in which they con their victims that they will double bank notes for them.
Source: http://www.khaleejtimes.com/DisplayArticle.asp?xfile=data/theuae/2004/April/theuae_April728.xml&section=theuae

8. *April 28, The Star−Telegram (TX)* — **Lubbock bank to acquire Fort Worth bank. State National Bancshares of Lubbock, TX is acquiring Fort Worth, TX−based Mercantile Bank Texas and looking for other acquisitions in the Fort Worth area. State National Bancshares Chief Executive Tom Nichols said Mercantile will keep its name.** The deal is expected to close in mid− to late July, pending regulatory approval, he said. Mercantile Bank had assets of a little more than $200 million as of December 31, according to the Federal Deposit Insurance Corporation and State National had more than $1.1 billion. Mercantile has operations in the growth areas of Arlington, Bedford, Fort Worth and Hurst, TX, which made it an attractive acquisition, Nichols said.
Source: http://www.dfw.com/mld/dfw/business/8539003.htm?1c

9. *April 28, General Accounting Office* — **GAO−04−307: Terrorism Insurance: Implementation of the Terrorism Risk Insurance Act of 2002 (Report).** After the terrorist attacks of September 11, 2001, insurance coverage for terrorism largely disappeared. Congress passed the Terrorism Risk Insurance Act (TRIA) in 2002 to help commercial property−casualty policyholders obtain terrorism insurance and give the insurance industry time to develop mechanisms to provide such insurance after the act expires on December 31, 2005. Under TRIA, the Department of Treasury caps insurer liability and would process claims and reimburse insurers for a large share of losses from terrorist acts that Treasury certified as meeting certain criteria. **As Treasury and industry participants have operated under TRIA for more than a year, the General Accounting Office (GAO) was asked to describe (1) their progress in implementing the act and (2) changes in the terrorism insurance market under TRIA. GAO recommends that the Secretary of the Treasury, as part of Treasury's study of the effectiveness of TRIA** and after consultation with insurance industry participants, identify for Congress alternatives that may exist for expanding the availability and affordability of terrorism insurance after TRIA expires. These alternatives could assist Congress during its deliberations about terrorism insurance. Highlights:
http://www.gao.gov/highlights/d04307high.pdf
Source: http://www.gao.gov/new.items/d04307.pdf

[Return to top]

Transportation Sector

10.

April 28, EurekAlert — **Airport baggage screeners may need continuing education, study indicates.** Baggage screeners have just seconds amid loud airport noises and the pressure of rushed airline travelers to scan X−rays of carry−on items for weapons. How good they are at finding one may depend on the specificity of their training, say researchers at the University of Illinois at Urbana−Champaign. **The findings, published in the May issue of the journal Psychological Science, suggest that initial training of federal airport screeners needs to last long enough for them to be exposed to a variety of weapons, and continuing education may be necessary to expose screeners to potentially new and unexpected ones.** The research was conducted at the Beckman Institute for Advanced Science and Technology at Illinois, using two−color X−ray images of carry−on baggage containing knives provided by the Federal Aviation Administration, which funded the study. Eye−tracking techniques captured where and how quickly the participants scanned through clothing, hair dryers, pill bottles and other items in each X−rayed piece of luggage to find a weapon.
Source: http://www.eurekalert.org/pub_releases/2004−04/uoia−abs04270 4.php

11. *April 28, Associated Press* — **California trains collide; no injuries reported. Two freight trains collided early Wednesday, April 28, near Hesperia, CA, leaving parts of two train cars dangling precariously over a cliff.** The trains, from Burlington Northern Santa Fe and Union Pacific Railroad, were on the same track and collided at 5:30 a.m., said Lena Kent, spokesperson for Burlington Northern. Five cars −− all from the Union Pacific train −− were damaged, she said. The trains carried no passengers and no injuries were reported, Kent said. **"The investigation will focus on why they were on the same track," Kent said, adding that the crews of both trains will undergo mandatory drug tests.** No hazardous materials were involved, she said. Some diesel fuel may have leaked from the Burlington Northern train. The trains carried a variety of freight, she said.
Source: http://www.usatoday.com/news/nation/2004−04−28−train−collisi on_x.htm

12. *April 28, Associated Press* — **High−speed ferry draws crowds in Rochester.** In Rochester, NY, a few thousand people lined the pier Tuesday, April 27, for their first glimpse of the Spirit of Ontario 1, an Australian−built, twin−hulled catamaran that could be the first of several deluxe, high−speed, car−and−passenger ferries plying the Great Lakes. **The 284−foot−long vessel is the world's most powerful diesel−powered catamaran.** It will make the lake crossing in about two hours and 15 minutes at up to 55 mph. The 171−mile road trip to Toronto usually takes three to four hours and far longer when there are miles−long backups at the border near Niagara Falls. "It's a very spectacular vessel designed for these parts," said Mayor William Johnson Jr. "I think a lot of people, now that it's here, are really going to overcome all of their doubts and we'll see tremendous use of this vessel. There's no question in my mind. **"You're going to see a resurgence of maritime travel, particularly around the Great Lakes, so I think Rochester will be a pioneer," Johnson predicted.** Two more high−speed car ferries will be launched in late spring −− one in Alaska, the other on Lake Michigan between Milwaukee, WI, and Muskegon, MI −− and itineraries are under review in Hawaii; Cleveland, OH; Erie, PA; Racine, WI, and along the East and West coasts.
Source: http://www.cnn.com/2004/TRAVEL/04/28/high.speed.ferry.ap/

13. *April 28, Associated Press* — **Former airport security employees charged with stealing from luggage. Four former employees of the Transportation Security Administration (TSA) have been charged with stealing and reselling laptop computers and other**

electronic devices from passengers' luggage at Detroit Metropolitan Airport. A federal grand jury on Tuesday indicted Tawann Alek Hayes, 21, of Westland; Shawn Edward Gordon, 21, of Southfield; Edwin Joshua Sturdivant, 22, of Detroit; and Joseph Byron Reynolds, 46, of Detroit. Reynolds was not a TSA employee at the time, but participated in the ring by reprogramming the computers and digital cameras for resale, the indictment states. The others were baggage screeners at the airport. The indictment alleges that from September 2003 through December 2003, the four men conspired to steal the electronics, erase the hard drives and reprogram them, and sell the stolen goods, U.S. Attorney Jeffrey Collins said in a statement.
Source: http://www.freep.com/news/statewire/sw96907_20040428.htm

[Return to top]

Postal and Shipping Sector

Nothing to report.
[Return to top]

Agriculture Sector

14. *April 28, Reuters* — **Future soy rust may cause one billion dollars in crop losses. U.S. farmers could lose between $640 million and $1.3 billion during the first year of a soybean rust outbreak should the disease hit the U.S. mainland, the U.S. Department of Agriculture (USDA) said on Tuesday, April 27.** An USDA economic analysis has concluded the wind−borne plant disease would eventually spread to the United States, probably from South America, and could cause some economic damage for many years after an initial outbreak. "The large range of damage estimates reflects the uncertainty associated with eventual effects of soybean rust in the United States," the report said. Soybean rust, which seriously erodes soybean plant yields, has never been reported in the continental United States. Hawaii was infected in 1994. The disease has cost farmers in Brazil billions of dollars. The USDA forecast that a U.S. outbreak would not be as severe, since soybean rust would probably become established only in the humid regions of the U.S. South. **USDA officials are weighing tougher import requirements for soymeal and soybeans from countries that already have soybean rust.** The report can be found at http://www.ers.usda.gov.
Source: http://www.agriculture.com/default.sph/AgNews.class?FNC=MonsentoDetail__ANewsindex_html___51663

15. *April 28, San Jose Mercury News* — **Sudden oak death found on East Coast. In the past two months, the microbe that causes sudden oak death has been found in 61 plant nurseries in nine states.** The spread started through shipments of plants from the giant wholesale Monrovia Nursery in Azusa, CA. It is not known how Monrovia's plants contracted sudden oak death. **Monrovia sent at least 292,500 plants susceptible to the fungus to 1,200 nurseries and retail outlets in 39 states during the period it was known to have the disease, according to the U.S. Department of Agriculture (USDA). And there is now evidence that Monrovia had shipped infected plants before the disease was discovered and could be stopped.** "There were plants that were shipped out to states that have traced back to sometime in early or

mid−2003 that were found to be positive," said Daniel J. Williams, the USDA's program manager for its National SOD Survey. "Information indicates that the infection existed prior to 2004" at Monrovia. Discovered nine years ago in an oak grove in Marin, CA, the fungus called Phytophthora ramorum has wiped out acres of forests in the most hard−hit region of the coastal Bay Area. It is not known how many of America's 80 varieties of oak trees, or other species of plants, would be vulnerable to sudden oak death. The southern live oaks, many alive since before the Civil War, are presumed to be susceptible to the disease.
Source: http://www.contracostatimes.com/mld/cctimes/news/state/85387 41.htm

16. *April 27, U.S. Department of Agriculture* — **Framework and funding for National Animal Identification System. Agriculture Secretary Ann M. Veneman Tuesday, April 27, announced the framework for implementation of a National Animal Identification System (NAIS) designed to identify any agricultural premise exposed to a foreign animal disease so that it can be more quickly contained and eradicated.** This announcement concludes several months of a U.S. Department of Agriculture (USDA) working group's efforts to develop an implementation framework for a U.S. animal identification plan. The implementation of a NAIS will be conducted in three main phases. **Under Phase I, USDA would evaluate current federally funded animal identification systems and determine which system(s) should be used for a NAIS, further the dialogue with producers and other stakeholders on the operation of a NAIS, identify staffing needs, and develop any regulatory and legislative proposals needed for implementing the system.** Phase II would involve the implementation of the selected animal identification system at regional levels for one or more selected species, continuation of the communication and education effort, addressing regulatory needs, and working with Congress on any needed legislation. In Phase III, the selected animal identification system(s) would be scaled up to the national level.
Source: http://www.usda.gov/Newsroom/0170.04.html

[Return to top]

Food Sector

17. *April 28, Agricultural Research Service* — **Bacterial proteins combat Campylobacter.** Proteins from harmless microorganisms can reduce Campylobacter and other pathogenic bacteria in poultry intestines, a team of Agricultural Research Service (ARS) and Russian scientists has discovered. ARS microbiologist Norman J. Stern used the proteins, called bacteriocins, to reduce Campylobacter numbers in bird intestines by 99.999 percent in small research trials. Large research trials will be necessary to determine if the technology is commercially feasible. **According to Stern, this is the first treatment used in the last 25 years to achieve a significant reduction of Campylobacter in research trials on chickens.** The bacteriocins reduce the numbers of Campylobacter by a millionfold when fed to chickens. Foodborne bacterial infections are responsible for billions of dollars of economic losses in the U.S. and worldwide. **The Centers for Disease Control and Prevention (CDC) notes that Campylobacter is one of the most common bacterial causes of diarrheal illness in humans in the United States. CDC has identified poultry as the primary vehicle for its transmission to humans.** Controlling Campylobacter in poultry would reduce public exposure to the bacteria.
Source: http://www.ars.usda.gov/News/docs.htm?docid=1261

18. *April 28, USA Today* — **Processors use tech to track meat progression. To fight foodborne disease, a Colorado slaughterhouse is using a high−tech computer system.** Most slaughterhouses in the U.S. process cattle about 20 at a time. Beef is usually identified with that lot number, but no more specific information about which cow it came from. If a piece of beef tests positive for a pathogen, everything in its lot usually must be recalled, says North Carolina State University professor Kevin Keener. Tracking tainted beef can be a race, since consumers usually eat beef not long after they buy it, Keener says. **The Colrado meatpacker hopes its new system, installed in its Greeley packing plant in November, will track a steak back to the cow it came from. That could limit the size and improve the speed of recalls.** The packer is using a new handheld scanning device. The packer starts by retinally scanning every cow, so each has a unique ID number. One plant worker scans the eye of each carcass as it zips by. The plant worker also scans in bar codes, RFID tags or other information. All that data is wirelessly transmitted to a computer. Tracking gets trickier when cows are prepared for butchering. The packer uses probability to match a steak with the ID number of the cow it came from. If the plant is butchering one cow every minute, the company knows that steaks cut between 2:15 and 2:16 probably come from a certain cow.
Source: http://www.usatoday.com/tech/news/techinnovations/2004−04−27−managingtech_x.htm

19. *April 27, MSNBC* — **FDA lists violators of mad cow feed rules. Just under 100 U.S. companies have recently violated regulations meant to prevent the spread of mad cow disease, according to new records from the Food and Drug Administration (FDA).** The FDA's database on feed inspections shows 12 recent cases, including a Kansas feed distributor, which the FDA said warranted its most serious action. Another 80 firms had minor violations. All of the dozen firms listed as FDA's most serious cases had problems noted during the past five months. **The violations included the potential for mixing prohibited material, as well as serious labeling or record−keeping problems, said Steve Solomon, of the FDA.** Federal officials insist one of the nation's best defenses against mad cow disease is the FDA's 1997 ban on feeding cattle protein or bone meal made from cows or other ruminants. "We still think it needs a lot of vigilance and we want to make sure nobody becomes complacent to the regulation. We think it is a credible firewall," Solomon said.
Source: http://msnbc.msn.com/id/4846765/

[Return to top]

Water Sector

20. *April 28, Washington Post* — **High lead found in Boston area water. Federal and state regulators ruled Tuesday, April 27, that the drinking water delivered to 2.5 million customers in the Boston region has lead levels above the acceptable national standard.** The ruling came after months of scrutiny by the U.S. Environmental Protection Agency and Massachusetts regulators who reviewed every water test conducted last year by the Massachusetts Water Resources Authority (MWRA). All water utilities must perform annual lead analyses to comply with the national Safe Drinking Water Act. The utility was seeking to invalidate tests from 18 households, most with high lead levels. Approval of the rare request would have allowed the utility to declare itself in compliance with federal law. After reviewing

the tests in the Boston region, the EPA and the state told the MWRA, the largest water utility in New England, that it could not invalidate the tests. The decision means the utility is considered to have high levels of lead in its water and is out compliance with federal law. **The high lead readings were concentrated in 10 of 28 suburban communities. MWRA officials said they expect that those 10 would have to begin replacing roughly seven percent of their lead service lines in the next year.**
Source: http://www.washingtonpost.com/wp−dyn/articles/A47845−2004Apr 27.html

21. *April 27, World Health Organization* — **Cleaner water saves lives and money, says UN. Meeting international development goals to halve the number of people who lack safe drinking water and adequate sanitation would repay the costs more than seven times over, according to a United Nations (UN) study.** The Swiss Tropical Institute, in a report commissioned by the World Health Organization (WHO), has outlined the significant economic benefits to the world, and particularly to developing countries, if the Millennium Development (MDG) and World Summit on Sustainable Development goals are met. In the report, Evaluation of the Costs and Benefits of Water and Sanitation Improvements at the Global Level, it is estimated that an additional investment of around $11.3 billion per year over and above current investments could result in a total economic benefit of $84 billion annually. The economic benefits would range from three dollars to $34 per one dollar invested, depending on the region.
Source: http://www.who.int/mediacentre/releases/2004/pr28/en/

[Return to top]

Public Health Sector

22. *April 28, BBC News* — **SARS cases in China. China has reported a new suspected case of the respiratory disease Severe Acute Respiratory Syndrome (SARS).** This brings the total to two confirmed SARS patients and seven suspected cases. The announcement comes as a World Health Organization (WHO) team began investigating how a graduate student was infected with SARS in a laboratory. **The WHO says about 1,000 people are now in isolation, but says that so far there is still no significant public health threat.** The latest suspected SARS case is a 49−year−old retired doctor, who shared a hospital room with another suspected SARS patient. The Ministry of Health says she is in critical condition. A WHO spokesman told the BBC he was concerned that infection is still occurring within hospitals.
Source: http://news.bbc.co.uk/2/hi/asia−pacific/3665979.stm

23. *April 28, Washington Post* — **Experimental smallpox vaccine protects monkeys from dying. Researchers at the U.S. Army laboratories at Fort Detrick in Frederick, MD, reported a major advance Tuesday, April 27, in the search for a safer smallpox vaccine. An experimental vaccine made from pieces of the live virus currently used as a smallpox vaccine protected monkeys against monkeypox, their version of the fatal illness.** The protection was not absolute, the animals got mildly ill and developed the characteristic pox rash, but it was good enough to keep them from dying. The new experiments, done in rhesus monkeys, suggest that a virtually risk−free subunit vaccine made from virus DNA might be an acceptable substitute for the old, whole−virus version.
Source: http://www.washingtonpost.com/wp−dyn/articles/A48089−2004Apr 27.html

24. *April 28, Xinhuanet* — **WHO calls for updated regulations to fight disease.** The World Health Organization (WHO) needs more powerful tools to fight the threat of emerging diseases such as Severe Acute Respiratory Syndrome (SARS) and avian influenza, a WHO official said Wednesday, April 28. **Most of the powers at WHO's disposal have become increasingly outdated, he said, leaving the global community at threat from pandemics and other health crises, said Shigeru Omi, WHO's Regional Director for the Western Pacific.** "The International Health Regulations (IHR) comprise the only internationally binding legislation on the reporting of epidemic diseases, but the need for updated regulations has been recognized for many years," Omi said. The IHR are the legal framework that governs WHO's work on the international spread of disease. Omi stressed the need to empower WHO to face the health challenges of the 21st century, noting that the present regulations are more than 30 years old. **"These regulations relate to an era when infectious diseases were on the decline," he said. Since then, the level of risk has risen significantly, driven by the "trinity" of organism, host, and environmental factors.**
Source: http://news.xinhuanet.com/english/2004−04/28/content_1445656 .htm

25. *April 28, Computer Weekly* — **Healthcare IT plan unveiled. President George W. Bush has unveiled a national healthcare IT plan focused on the development of personal electronic medical records and the appointment of a health care IT tsar to oversee the process.** Bush called the existing paper−based U.S. medical record system antiquated and said "medicine ought to be using modern technologies in order to better share information, to reduce medical errors and cost to our health care system by billions of dollars." The White House said that the adoption of standards is key to development of a portable, electronic medical record. Last July, the Department of Health and Human Services (HHS) launched a program to provide a standardized clinical terminology database to healthcare organizations nationwide. That database will serve as one of the building blocks of a electronic medical record. **Standards will enable transmission of X−rays over the Internet, aid transmission of electronic lab results, and lead to the development of electronic prescriptions.**
Source: http://www.computerweekly.com/articles/article.asp?liArticleID=130220&liArticleTypeID=1&liCategoryID=2&liChannelID=20&liFlavourID=1&sSearch=&nPage=1

[Return to top]

Government Sector

26. *April 28, Government Computer News* — **DHS council to propose online lexicon. The Department of Homeland Security's (DHS) Advisory Council plans to recommend that the department post an online lexicon of important terms used in the homeland security field to help officials and the public avoid confusion when discussing key concepts.** Christopher Furlow, the council's executive director, said the proposal would go to Homeland Security Secretary Tom Ridge in a matter of days. "With some folks, their eyes glaze over when you first start talking about lexicon," Furlow said. "But all it takes is a few examples." He described how the acronym CERT can refer to a computer emergency response team, a civil emergency response team or a community emergency response team. "That describes entities that would have vastly different roles in an emergency," he said. **A more recent example is the**

acronym RDD, which in the past mainly was used to refer to radiological dispersion devices. “But in the wake of the Madrid bombings, you see it being used to describe remote detonation devices,” Furlow said. “Certainly if you are a first responder, seeing RDD is going to influence how you respond.” Furlow said the council would recommend that DHS hire a lexicographer to gather key acronyms and terms from important documents and maintain an online database that would be available to the public and updated continuously.
Source: http://www.gcn.com/vol1_no1/homeland−security/25764−1.html

[Return to top]

Emergency Services Sector

27. *April 28, TheBostonChannel.com* — **Ferry officials prep for possible attack.** NewsCenter 5's Jack Harper reported that the scene looked like the worst scenario −− terrorists taking control of a ferry at Woods Hole, MA. **Luckily, it was a drill for local, state and federal agencies to prepare for something they hope they never see. "We're seeing several mini−scenarios: a potential port security risk, the attempted take over of a ferry by a terrorist, the second attempt with a weapon of mass destruction," said U.S. Coast Guard Capt. Mary Landry.** Ferries operating in southeastern Massachusetts and Rhode Island move more than three million people a year. As they approach their business season, there is more emphasis then ever before on security. "I think they'll notice very little difference in their traveling. They will see more police presence on some weekends. There will be random checks of some vehicles. But I hope our new transportation policies will be transparent," said the Steamship Authority's Paul Peters. Tuesday's drills focused on training for the worst−case scenario, but officials hope if all the other less obvious prevention is successful, their training will not be needed.
Source: http://www.thebostonchannel.com/news/3243118/detail.html

28. *April 28, The News−Sentinel (Ft. Wayne, IN)* — **Federal grants to replace defective gas masks.** After the September 11, 2001, attacks, Indiana bought about 16,000 gas masks to protect emergency workers from chemical or biological attacks. As it turns out, the decision wasted millions of dollars −− and might risk lives, as well. **In the rush to equip police, fire, medical and other agencies that would respond to terror attacks, the state bought masks that were not approved by federal and state safety agencies for protection against chemical and biological attacks.** The masks purchased were made of silicone, not rubber −− meaning they could be eaten away in contact with certain chemicals. The original hoods may still be useful for responding to some emergencies, such as a train derailment that causes the spill of a known chemical.
Source: http://www.fortwayne.com/mld/fortwayne/news/local/8541444.ht m

[Return to top]

Information Technology and Telecommunications Sector

29. *April 28, TechWeb* — **Netsky.x lays out Websites.** The Netsky.x worm, which hit the Internet over a week ago and targeted a trio of educational Websites for denial−of−service (DoS) attacks, has laid low two of the three in the first day of its scheduled three−day assault. **Version**

X of the persistent Netsky worm launched a DoS attack on nibis.de, medinfo.ufl.edu, and educa.ch, educational sites from Germany, the United States, and Switzerland, respectively. The DoS attacks, which began Wednesday, April 28, by Netsky.x−infected computers, and is to run through Friday, effectively shut down the German and U.S. sites, according to Ken Godskind of AlertSite, a Web monitoring firm. Other variants released after Netsky.x−−including Netsky.y and Netsky.z−−also targeted the three sites for DoS attacks that could run as long as May 5. The two most recent Netskys, however, dubbed Netsky.aa and Netsky.ab −− which appeared Monday and today, respectively, don't take aim at the educational sites. Instead, **Netsky.ab tries to delete the entries of several variations of its rival, Bagle, from the Windows Registry.**
Source: http://www.techweb.com/wire/story/TWB20040428S0006

30. *April 28, vnunet.com (UK)* — **UK businesses still vulnerable to security breaches.** A lack of IT security skills is leaving UK businesses vulnerable to security breaches, according to research. **The Department of Trade and Industry Information Security Breaches Survey 2004 suggests that 89 per cent of companies say staff have no formal IT security qualifications.** The study, by PricewaterhouseCoopers (PwC), says there is an average of one security incident per month in UK firms, but one a week in large companies. Three−quarters of UK companies, and 94 per cent of large organisations, suffered a security incident in the last year. **Human error is the cause of most problems, but only a third of businesses have a security policy in place.** Security spending has increased since the last survey in 2002, but only slightly from two per cent to three per cent of the annual IT budget. The report says this is well below the five to 10 per cent benchmark level. The study is available online: http://www.security−survey.gov.uk/
Source: http://www.vnunet.com/News/1154752

31. *April 27, Reuters* — **UK to review cybercrime law.** Britain is to update its lone cybercrime law. Organized gangs around the world are honing their hacking, spamming and virus−writing skills while thinly stretched police resources are struggling to cope. **The legal update will be closely watched by other countries, many of whose own laws against cybercrime are considered insufficient to fight what has become one of the fastest growing global crime waves.** A group of parliamentarians will hold a public debate on Thursday, April 29, to explore ways to bring the Computer Misuse Act, or CMA, into the Internet era. Working with the UK's Home Office, the aim is to have a new cybercrime bill introduced in the next six months, MP Brian White said. Police say cybercrime costs UK industry hundreds of millions, and perhaps billions, of pounds annually. Globally, the figure is staggering, law enforcement officials say. **"Serious and organized crime groups, and potentially terrorists, are moving into cyberspace simply because it's easier to hide there**," said Simon Moores, a computer crime expert who works with the UK government. Thin resources, few convictions The need for an updated law is most evident to prosecutors and police. The Home Office said there were just 14 convictions under the CMA in 2002, the last year statistics were tallied.
Source: http://www.cnn.com/2004/TECH/internet/04/27/crime.britain.in ternet.reut/index.html

32. *April 26, Network World* — **User group defines security needs. The Network Applications Consortium (NAC) plans to publish a document this summer that outlines the principle, policies, standards, technologies and processes necessary to protect a company's information assets**. NAC's Enterprise Security Architecture addresses hot topics in

cybersecurity such as governance, technology architecture and operations. The document will affect how several major corporations−−including Bechtel, Boeing, GlaxoSmithKline and State Farm Insurance−−make network hardware and software purchases in the future, network executives at these companies say. NAC members also plan to use the document to influence how key network vendors such as Cisco, Entrust, Microsoft and Symantec create security products. The consortium plans to embrace several security standards−−selections have not been finalized−−and urge vendors to adopt these standards. The document's goal is to create a framework that lets companies mix and match security products from different vendors while assuring interoperability and manageability. Additional information is available on the NAC Website: http://www.netapps.org/
Source: http://www.nwfusion.com/news/2004/0426nac.html

Internet Alert Dashboard

Current Alert Levels

AlertCon: 2 out of 4 https://gtoc.iss.net	Security Focus ThreatCon: 2 out of 4 http://analyzer.securityfocus.com/

Current Virus and Port Attacks

Virus:	#1 Virus in the United States: **HTML_NETSKY.P** Source: http://wtc.trendmicro.com/wtc/wmap.html, Trend World Micro Virus Tracking Center [Infected Computers, North America, Past 24 hours, #1 in United States]
Top 10 Target Ports	3127 (mydoom), 1025 (blackjack), 6129 (dameware), 4899 (radmin), 2745 (Bagle.C), 1026 (nterm), 1434 (ms−sql−m), 135 (epmap), 1433 (ms−sql−s), 80 (www) Source: http://isc.incidents.org/top10.html; Internet Storm Center

[Return to top]

General Sector

33. *April 28, New York Times* — **Damascus hit by a bombing and a gunfight.** Heavily armed assailants detonated a bomb near a cluster of foreign embassies in Damascus, the Syrian capital, on Tuesday, April 28, setting off an intense gun battle with state security forces that maintain exceptionally tight control over the society. Early Wednesday, Syrian television reported that security forces had found a cache of arms and explosives in a raid in the upscale Damascus district where the police had clashed with the gunmen. An unidentified Interior Ministry official quoted by the Syrian news agency SANA said one officer and a woman who was passing by were killed in the shootout. The official said two of the attackers had also been killed. **In Syria, violence like this has been nearly unheard of for two decades. The government has a history of crushing any sign of Islamic radicalism within its borders, although it has been accused by the United States of sponsoring terrorism in Lebanon and Israel**. American

officials also accuse Syria of allowing foreign fighters to cross from its territory into Iraq to attack allied occupation forces. The British, Canadian and Iranian Embassies are in the area of the attack. A British Foreign Office spokesman in London said none of its nationals had been hurt. Canadian officials, however, said their embassy had been slightly damaged in the fighting.
Source: http://www.nytimes.com/2004/04/28/international/middleeast/2 8SYRI.html

34. *April 28, Newsday.com* — **Powder found in Clinton's office mail.** A Secret Service agent assigned to former President Bill Clinton requested to be decontaminated at his Harlem office Tuesday, April 27, after he opened a package containing a vial of white powder, sources said. **The agent was screening Clinton's mail as part of a routine procedure in the first−floor mailroom at 55 W. 125th St. when he opened a box and discovered the vial and an accompanying letter, sources said.** He contacted the Police Department, which responded with a Hazmat team and Emergency Services Units. The Department of Environmental Protection and the city's Department of Health also sent inspectors to run preliminary tests. Those tests came back negative, sources said. A spokesman for the Department of Health said additional tests would be conducted at the department's Manhattan laboratories to determine whether the substance is anthrax or another biological agent.
Source: http://www.newsday.com/news/local/newyork/nyc−nyclin28377699 6apr28,0,7172332.story?coll=ny−nynews−headlines

[Return to top]

DHS/IAIP Products &Contact Information

The Department of Homeland Security's Information Analysis and Infrastructure Protection (IAIP) serves as a national critical infrastructure threat assessment, warning, vulnerability entity. The IAIP provides a range of bulletins and advisories of interest to information system security and professionals and those involved in protecting public and private infrastructures. By visiting the IAIP web−site (http://www.nipc.gov), one can quickly access any of the following DHS/IAIP products:

DHS/IAIP Warnings − DHS/IAIP Assessements, Advisories, and Alerts: DHS/IAIP produces three levels of infrastructure warnings. Collectively, these threat warning products will be based on material that is significant, credible, timely, and that address cyber and/or infrastructure dimensions with possibly significant impact.

DHS/IAIP Publications − DHS/IAIP Daily Reports, CyberNotes, Information Bulletins, and other publications

DHS/IAIP Daily Reports Archive − Access past DHS/IAIP Daily Open Source Infrastructure Reports

DHS/IAIP Daily Open Source Infrastructure Report Contact Information

Content and Suggestions:	Send mail to dhsdailyreport@mail.dhs.osis.gov or contact the DHS/IAIP Daily Report Team at (703) 883−3644.
Subscription and Distribution Information:	Send mail to dhsdailyreport@mail.dhs.osis.gov or contact the DHS/IAIP Daily Report Team at (703) 883−3644 for more information.

Contact DHS/IAIP

To report physical infrastructure incidents or to request information, please contact the National Infrastructure Coordinating Center at nicc@dhs.gov or (202) 282−9201.

To report cyber infrastructure incidents or to request information, please contact US−CERT at info@us−cert.gov or visit their Web page at www.uscert.gov.

DHS/IAIP Disclaimer

The DHS/IAIP Daily Open Source Infrastructure Report is a daily [Monday through Friday] summary and assessment of open−source published information concerning significant critical infrastructure issues. This is an internal DHS/IAIP tool intended to serve the informational needs of DHS/IAIP personnel and other interested staff. Further reproduction or redistribution for private use or gain is subject to original copyright restrictions of the content. The IAIP provides no warranty of ownership of the copyright, or of accuracy in respect of the original source material.